Amendments to the Claims:

This listing of the claims will replace all prior versions and listings of claims in the application.

Listing of Claims:

1. (currently amended) A method for securely delivering content over a network comprising:

(a) storing at least one title on a content server operatively coupled to the network, the title stored in unexecutable form;

(b) storing on an access server operatively coupled to the network a location identifier of the title [and] as well as data [necessary] unique to the title to process the title into executable form;

(c) requiring a client process operatively coupled to the network to obtain the location identifier of the title from the access server prior to retrieving at least a portion of the title from the content server; and

(d) requiring a client process to obtain from the access server the data [necessary] unique to the title to process the portion of the title into executable form.

2. (previously presented) The method of claim 1 further comprising:

(e) requiring the client process to obtain a signature of the access server and to present the signature to the content server before retrieving at least a portion of the title from the content server.

3. (previously presented) The method of claim 1 further comprising:

(e) requiring the client process to obtain from the access server time data defining a time period in which the client process may retrieve at least a portion of the title from the content server.

4. (previously presented) The method of claim 3 further comprising:

(f) requiring the client process to obtain new time data from the access server once the time period has expired and before retrieving at least a portion of the title from the content server.

5. (previously presented) The method of claim 2 further comprising:

(f) requiring the client process to obtain new time data from the access server once an initial time period has expired and before retrieving at least a portion of the title form the content server.

6. (currently amended) An apparatus for secure delivery of content over a network comprising:

(a) a content server operatively coupled to the network and having at least one title stored therein in unexecutable form;

(b) an access server operatively coupled to the network and having stored therein a location identifier of the title [and] as well as data [necessary] unique to the title to process at least a portion of the title into executable form; and

(c) a client system operatively coupled to the network and containing program logic configured to obtain from the access server the location identifier of the title and the data [necessary] unique to the title to process the portion of the title into executable form.

7. (original) The apparatus of claim 6 wherein the client system further comprises:
program logic configured to execute portion of the title.

8. (original) The apparatus of claim 6 wherein the access server further comprises:
program logic configured to generate time data defining a time period in which the client system may retrieve at least a portion of the title from the content server.

9. (original) The apparatus of claim 8 wherein the client system further comprises:
program logic configured to request new time data from the access server once the time period has expired.

10. (original) The apparatus of claim 6 wherein the network comprises a broadband access network.

11. (previously presented) Apparatus for secure delivery of content over a network comprising:

(A) a content server comprising a processor, a memory and a network interface for operatively coupling the content server to the network, the content server further comprising:

(A.1) authentication logic, responsive to a token received from a client process, the token containing data identifying a time period, and configured to determine whether the client process is authorized to access the memory at a specific time; and

(A.2) access logic, responsive to the token received from the client process, the token containing data uniquely identifying one of the titles stored in the memory, and configured to enable access to the memory and the title uniquely identified by the token;

C1

(B) an access server comprising a processor, a memory and a network interface for operatively coupling the access server to the network, the access server further comprising:

(B.1) conversion logic, responsive to a unique identifier of a title supplied by a client process and configured to convert the unique identifier of the title into a location identifier indicating an address on the network where the title may be accessed; and

(B.2) activator generation logic responsive to a request from a client process and configured to generate an activator in response thereto; and

(C) a client system comprising a processor, a memory and a network interface for operatively coupling the client system to the content server and the access server over the network, the client system further comprising:

(C.1) program logic configured to obtain from the access server a token, an activator and a location identifier of the content server at which an identified title can be accessed;

(C.2) program logic configured to retrieve at least a portion of the identified title from the content server; and

(C.3) program logic configured to execute the portion of the identified title retrieved from the content server.

12. (currently amended) The apparatus of claim 11 wherein the client system further comprises an operating system executable on the processor[[,]] and wherein the client system further comprises:

(C.4) program logic configured to mount a network file system associated with the identified title and store in the memory of the client system, a plurality of registry entries related to the title;

(C.5) program logic configured to intercept requests form the operating system during title execution and redirect selected of the intercepted request to the set of registry entries.

13. (original) The apparatus of claim 11 wherein the activator comprises cryptographic data.

14. (original) The apparatus of claim 11 wherein the activator comprises at least one bytecode and the client system further comprises:

(C.4) program logic configured to interpret and execute the bytecode contained within the activator.

15. (original) The apparatus of claim 14 wherein the token comprises data identifying the access server which generated the token.

16. (original) The apparatus of claim 11 wherein the activator further comprises authorization data.

17. (original) The apparatus of claim 11 wherein the token further comprises:
start time data and end time data which collectively define a time period.

18. (original) The apparatus of claim 11 wherein the title is stored in the memory of the content server in the form of a briq.

19. (original) The apparatus of claim 11 wherein the briq comprises at least one file containing data comprising at least a portion of a title.

20. (original) The apparatus of claim 11 wherein the network comprises a broadband access network.

21. (previously presented) A system for delivery of content to a client system over a network, comprising:

a content server operatively coupled to the network and having at least one content title stored therein in unexecutable form; and

an access server operatively coupled to the network and having stored therein a location identifier of the content title and data for processing at least a portion of the content title into executable form, the access server having program logic configured to provide the location identifier of the content title and the data for processing the portion of the content title into executable form to the client system.

22. (previously presented) The system of claim 21, wherein the content server comprises program logic responsive to a token received from the client system containing data identifying a content title stored on the content server, the program logic enabling access to at least a portion of the content title identified by the token.

23. (previously presented) The system of claim 22, wherein the program logic of the content server authenticates the content title identification data on the token prior to enabling access to the content title.

24. (previously presented) The system of claim 22, wherein the token specifies a time period for providing access to the content title identified by the token, the program logic of the content server being configured to enable access to at least a portion of the identified content title only during the time period specified by the token.

25. (previously presented) The system of claim 24, wherein the token further contains data specifying a start time and an end time defining the specified time period.

26. (previously presented) The system of claim 21, wherein the access server further comprises token generating logic configured to generate a token containing data identifying a content title requested by the client system and data specifying a time period for accessing the requested content title from the content server.

27. (previously presented) The system of claim 26, wherein the token generating logic provides the token with a start time and an end time specifying the time period for accessing the requested content title.

28. (previously presented) The system of claim 26, wherein the token generating logic provides the token with data identifying the access server.

29. (previously presented) The system of claim 26, wherein the access server further comprises conversion logic configured to convert an identifier of a content title supplied by the client system into a location identifier indicating an address on the network where the content title might be found.

30. (previously presented) The system of claim 21, wherein the access server further comprises activator generator logic for generating an activator containing the data necessary to process at least a portion of the content title into executable form.

31. (previously presented) The system of claim 30, wherein the data necessary to process at least a portion of the content title into executable form includes cryptographic data.

32. (previously presented) The system of claim 31, wherein the cryptographic data is embedded in obfuscated bytecode.

33. (previously presented) A method of processing content into a file package suitable for delivery across a network, the method comprising:

extracting registry information about a content title, the registry information corresponding to one or more selected data files of the content title,

storing the registry information in a registry entry file,

encrypting the registry entry file and at least a portion of the corresponding data files of the content title, and

storing the encrypted files in a file package at a location on a network file system.

34. (previously presented) The method of claim 33, wherein the registry information includes at least one of the file names, the directory names, and the configuration settings for execution of the selected data files.

35. (previously presented) The method of claim 33, further comprising

creating a header for the file package, the header identifying at least one of the title, the location of the file package on the network, the system requirements for the content title, the names of the encrypted data files, and a map of the network mountable file system.

36. (previously presented) The method of claim 35, further comprising

storing the header at the location of the file package.

37. (previously presented) The method of claim 35, wherein the header is unencrypted.

38. (previously presented) The method of claim 33, further comprising

creating a cryptographic block providing data concerning the encryption of the encrypted files of the file package.

39. (previously presented) The method of claim 38, wherein the encryption data comprises data identifying at least one of the key version and the type of encryption used.

40. (currently amended) In a system for delivery of a content title to a client system over a computer network, the system including a content server having at least one content title stored thereon in unexecutable form, a method for creating an activator for processing a content title into executable form, comprising

providing cryptographic data for decrypting content title data,

embedding the encryption data in obfuscated bytecode to inhibit unauthorized extraction of the cryptographic data, and

storing the activator in the form of the obfuscated bytecode at a location on the computer network accessible by the client system .

41. (currently amended) The method of claim [[~~41~~]] 40, further comprising

adding authorization data to the activator, the authorization data identifying a time period in which the content title remains in executable form.

42. (previously presented) The method of claim 41, further comprising

creating a token authorizing the client system to access a content title stored on the content server, and

storing the token with the activator at a location on the computer network accessible by the client system.